Home Depot breach affected 56M debit, credit cards (Update)

September 18 2014, by Anne D'innocenzio

In this Feb. 22, 2010 file photo, shoppers walk through the aisles at the Home Depot store in Williston, Vt. The Home Depot on Thursday, Sept. 18, 2014 said it has eliminated malware from its U.S. and Canadian networks that affected 56 million unique payment cards between April and September. (AP Photo/Toby Talbot, File)

Home Depot said Thursday that a data breach that lasted for months at its stores in the U.S. and Canada affected 56 million debit and credit cards, far more than a pre-Christmas 2013 attack on Target customers.

The size of the theft at Home Depot trails only that of TJX Companies' heist of 90 million records disclosed in 2007. Target's breach compromised 40 million credit and debit cards.

Home Depot, the nation's largest home improvement retailer, said that the malware used in the data breach that took place between April and September has been eliminated.

It said there was no evidence that debit PIN numbers were compromised or that the breach affected stores in Mexico or customers who shopped online at Homedepot.com. It said it has also completed a "major" payment security project that provides enhanced encryption of customers' payment data in the company's U.S. stores.

But unlike Target's breach, which sent the retailer's sales and profits falling as wary shoppers went elsewhere, customers seem to have stuck with Atlanta-based Home Depot. Still, the breach's ultimate cost to the company remains unknown. Greg Melich, an analyst at International Strategy & Investment Group LLC, estimates the costs will run in the several hundred million dollars, similar to Target's breach.

"This is a massive breach, and a lot of people are affected," said John Kindervag, vice president and principal analyst at Forrester Research. But he added, "Home Depot is very lucky that Target happened because there is this numbness factor."

Customers appear to be growing used to breaches, following a string of them this past year, including at Michaels, SuperValu and Neiman Marcus. Home Depot might have also benefited from the disclosure of the breach coming in September, months after the spring season, which is the busiest time of year for home improvement.

And unlike Target, which has a myriad of competitors, analysts note that

home-improvement shoppers don't have many options. Moreover, Home Depot's customer base is different from Target's. Nearly 40 percent of Home Depot's sales come from professional and contractor services. Those buyers tend to be fiercely loyal and shop a couple of times a week for supplies.

Home Depot on Thursday confirmed its sales-growth estimates for the fiscal year and said it expects to earn $4.54 per share in fiscal 2014, up 2 cents from its prior guidance. The company's fiscal 2014 outlook includes estimates for the cost to investigate the data breach, providing credit monitoring services to its customers, increasing call center staffing and paying legal and professional services.

However, the profit guidance doesn't include potential yet-to-be determined losses related to the breach. The company said it has not yet estimated costs beyond those included in the guidance issued Thursday. Those costs could include liabilities related to payment card networks for reimbursements of credit card fraud and card reissuance costs. It could also include future civil litigation and governmental investigations and enforcement proceedings.

"We apologize to our customers for the inconvenience and anxiety this has caused, and want to reassure them that they will not be liable for fraudulent charges," Home Depot's chairman and CEO, Frank Blake, said in a statement. "From the time this investigation began, our guiding principal has been to put our customers first, and we will continue to do so."

The breach at Home Depot was first reported on Sept. 2 by Brian Krebs of Krebs on Security, a website that focuses on cybersecurity.

Target's high-profile breach pushed banks, retailers and card companies to increase security by speeding the adoption of microchips in U.S.

credit and debit cards. Supporters say chip cards are safer, because unlike magnetic strip cards that transfer a credit card number when they are swiped at a point-of-sale terminal, chip cards use a one-time code that moves between the chip and the retailer's register. The result is a transfer of data that is useless to anyone except the parties involved. Chip cards are also nearly impossible to copy, experts say.

Target has been overhauling its security department and systems and is accelerating its $100 million plan to roll out chip-based credit card technology in all of its nearly 1,800 stores. Home Depot said it will be activating chip-enabled checkout terminals at all of its U.S. stores by the end of the year.